CLAIMS

1. A method for checking a model, which defines states of a system under study and a transition relation among the states, the method comprising:

specifying a property that applies to a target set that comprises at least one target state among the states of the system under study;

beginning from an initial set of at least one initial state among the states of the system, computing successive reachable sets comprising the states of the system that are reachable from the initial set;

finding an intersection between one of the reachable sets and the target set; and

computing a plurality of mutually-disjoint traces from the at least one target state in the intersection through the states in the reachable sets to the at least one initial state.

2. A method according to claim 1, wherein specifying the property comprises specifying a condition that is expected to be true over all of the reachable states of the system under study, and wherein the condition is false in the at least one target state.

3. A method according to claim 1, wherein specifying the property comprises specifying a condition representing a desired behavior of the system under study, such that the condition is fulfilled in the at least one target state.

4. A method according to claim 1, wherein computing the successive reachable sets comprises testing the property

while computing the sets, and ceasing to compute the sets when the intersection is found.

5. A method according to claim 1, wherein computing the successive reachable sets comprises:

determining a first one of the reachable sets, disjoint from the initial set, such that all of the states in the first one of the reachable sets are reached from the at least one initial state in a first cycle of the transition relation; and

determining the successive reachable sets, following the first one of the reachable sets, such that all of the states in each of the reachable sets are reached from the states in a preceding one of the reachable sets in a successive cycle of the transition relation, and so that each of the successive reachable sets is disjoint from the initial set and from the other reachable sets determined before it.

6. A method according to claim 5, wherein computing the traces comprises, for each trace among the multiple traces, selecting one of the states from each of the successive reachable sets.

7. A method according to claim 6, wherein selecting the one of the states comprises, for each of the selected states, choosing a predecessor state among the states in a preceding one of the reachable sets until the state on the trace in the first one of the reachable sets is found, and choosing the predecessor state in the initial set to the state in the first one of the reachable sets.

8. A method according to claim 7, wherein choosing the predecessor state comprises, on each of the traces

computed after a first one of the traces, choosing the predecessor state so as to maximize a distance of the trace from the other traces already computed.

9. A method according to claim 1, wherein computing the traces comprises selecting the states on each trace among the multiple traces so as to maximize a distance of the trace from the other traces already computed.

10. A method according to claim 9, wherein each of the states is represented by a binary decision diagrams (BDD), and wherein selecting the states on each trace comprises maximizing the distance between the BDD representing the state to be selected and the BDD representing the states on the other traces.

11. A method according to claim 10, wherein maximizing the distance comprises:

taking a left trial state and a right trial state on left and right branches, respectively, of the BDD representing the state to be selected; and

choosing the trial state that has a larger Hamming distance from the BDD representing the states on the other traces.

12. Model checking apparatus, comprising a model processor, which is arranged to receive a model defining states of a system under study and a transition relation among the states, and to receive a specification of a property that applies to a target set comprising at least one target state among the states of the system under study, the processor being further arranged to compute, beginning from an initial set of at least one initial state among the states of the system, successive

reachable sets comprising the states of the system that are reachable from the initial set, to find an intersection between one of the reachable sets and the target set, and to compute a plurality of mutually-disjoint traces from the at least one target state in the intersection through the states in the reachable sets to the at least one initial state.

13. Apparatus according to claim 12, wherein the property comprises a condition that is expected to be true over all of the reachable states of the system under study, and wherein the condition is false in the at least one target state.

14. Apparatus according to claim 12, wherein the property comprises a condition representing a desired behavior of the system under study, such that the condition is fulfilled in the at least one target state.

15. Apparatus according to claim 12, wherein the processor is arranged to test the property while computing the sets, and ceases to compute the sets when the intersection is found.

16. Apparatus according to claim 12, wherein the processor is arranged to compute a first one of the reachable sets, disjoint from the initial set, such that all of the states in the first one of the reachable sets are reached from the at least one initial state in a first cycle of the transition relation, and further to compute the successive reachable sets, following the first one of the reachable sets, such that all of the states in each of the reachable sets are reached from the states in a preceding one of the reachable sets in a

successive cycle of the transition relation, and so that each of the successive reachable sets is disjoint from the initial set and from the other reachable sets determined before it.

17. Apparatus according to claim 16, wherein the processor is arranged to compute the traces by selecting, for each trace among the multiple traces, one of the states from each of the successive reachable sets.

18. Apparatus according to claim 17, wherein the processor is arranged to compute the traces by choosing, for each of the selected states, a predecessor state among the states in a preceding one of the reachable sets until the state on the trace in the first one of the reachable sets is found, and choosing the predecessor state in the initial set to the state in the first one of the reachable sets.

19. Apparatus according to claim 18, wherein the processor is arranged to choose the predecessor state on each of the traces computed after a first one of the traces so as to maximize a distance of the trace from the other traces already computed.

20. Apparatus according to claim 12, wherein the processor is arranged to compute the traces by selecting the states on each trace among the multiple traces so as to maximize a distance of the trace from the other traces already computed.

21. Apparatus according to claim 20, wherein each of the states is represented by a binary decision diagrams (BDD), and wherein the processor is arranged to select the states on each trace so as to maximize the distance

between the BDD representing the state to be selected and the BDD representing the states on the other traces.

22. Apparatus according to claim 21, wherein the processor is arranged to maximize the distance by taking a left trial state and a right trial state on left and right branches, respectively, of the BDD representing the state to be selected, and choosing the trial state that has a larger Hamming distance from the BDD representing the states on the other traces.

23. A computer software product, comprising a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to receive a model defining states of a system under study and a transition relation among the states, and to receive a specification of a property that applies to a target set comprising at least one target state among the states of the system under study, the instructions further causing the computer to compute, beginning from an initial set of at least one initial state among the states of the system, successive reachable sets comprising the states of the system that are reachable from the initial set, to find an intersection between one of the reachable sets and the target set, and to compute a plurality of mutually-disjoint traces from the at least one target state in the intersection through the states in the reachable sets to the at least one initial state.

24. A product according to claim 23, wherein the property comprises a condition that is expected to be true over all of the reachable states of the system under

study, and wherein the condition is false in the at least one target state.

25. A product according to claim 23, wherein the property comprises a condition representing a desired behavior of the system under study, such that the condition is fulfilled in the at least one target state.

26. A product according to claim 23, wherein the instructions cause the computer to test the property while computing the sets, and to cease to compute the sets when the intersection is found.

27. A product according to claim 23, wherein the instructions cause the computer to compute a first one of the reachable sets, disjoint from the initial set, such that all of the states in the first one of the reachable sets are reached from the at least one initial state in a first cycle of the transition relation, and further to compute the successive reachable sets, following the first one of the reachable sets, such that all of the states in each of the reachable sets are reached from the states in a preceding one of the reachable sets in a successive cycle of the transition relation, and so that each of the successive reachable sets is disjoint from the initial set and from the other reachable sets determined before it.

28. A product according to claim 27, wherein the instructions cause the computer to compute the traces by selecting, for each trace among the multiple traces, one of the states from each of the successive reachable sets.

29. A product according to claim 28, wherein the instructions cause the computer to compute the traces by

choosing, for each of the selected states, a predecessor state among the states in a preceding one of the reachable sets until the state on the trace in the first one of the reachable sets is found, and choosing the predecessor state in the initial set to the state in the first one of the reachable sets.

30. A product according to claim 29, wherein the instructions cause the computer to choose the predecessor state on each of the traces computed after a first one of the traces so as to maximize a distance of the trace from the other traces already computed.

31. A product according to claim 23, wherein the instructions cause the computer to compute the traces by selecting the states on each trace among the multiple traces so as to maximize a distance of the trace from the other traces already computed.

32. A product according to claim 31, wherein each of the states is represented by a binary decision diagrams (BDD), and wherein the instructions cause the computer to select the states on each trace so as to maximize the distance between the BDD representing the state to be selected and the BDD representing the states on the other traces.

33. A product according to claim 21, wherein the instructions cause the computer to maximize the distance by taking a left trial state and a right trial state on left and right branches, respectively, of the BDD representing the state to be selected, and choosing the trial state that has a larger Hamming distance from the BDD representing the states on the other traces.